WHAT IS CLAIMED IS:

1. A machine-implemented method comprising:

producing a first authentication message comprising:

authentication data encrypted with a first key; and

a data structure comprising the first key, wherein the data structure is encrypted with a second key;

generating a request message to have a first network device associated with a first network deliver datagrams destined for a home address associated with a mobile device on the first network to a second address on a second, different network; and

embedding the authentication message in the request message.

2. The method of claim 1 wherein the authentication data comprises a timestamp.

3. The method of claim 1 wherein the second key is known to the first network device and unknown to the mobile node.

4. The method of claim 1 wherein the authentication message comprises a Kerberos Application Request.

5. The method of claim 1 wherein the data structure comprises a Kerberos ticket.

6. The method of claim 1 further comprising generating a second authentication message.

7. The method of claim 6, wherein generating a second authentication message comprises:

generating a hash of the request message using the first key.

8. The method of claim 6 further comprising:

transmitting the request message and second authentication message to the first network device.

9. The method of claim 8 further comprising:

receiving the request message and second authentication message by a device on the home network; and

decrypting the data structure using the second key to obtain the first key.

10. The method of claim 9 further comprising:

verifying the second authentication message using the first key.

11. The method of claim 9 further comprising generating a third key.

12. The method of claim 9 further comprising generating key material, wherein the key material may be supplied to a function to generate a third key.

13. The method of claim 1 wherein the request message comprises a Registration Request message.

14. The method of claim 11 further comprising:

forming a reply authentication message comprising the third key encrypted with the first key.

15. The method of claim 14 wherein the reply authentication message comprises a Kerberos Application Reply message.

16. The method of claim 14 further comprising:

forming a reply message that includes the reply authentication message.

17. The method of claim 16 wherein the reply message comprises a Registration Reply message.

18. The method of claim 16 further comprising:

generating a third authentication message; and

transmitting the reply message and third authentication message to the mobile node.

19. The method of claim 18 wherein generating a third authentication message comprises:

generating a hash of the reply authentication message using the first key.

20. A machine-implemented method comprising:

receiving at a first device associated with a home network an authentication message and a request message to reroute datagrams destined for a first address of a mobile device associated with the home network to a second address not associated with the home network, wherein the request message comprises:

a data structure that includes a first key encrypted with a second key; and

determining if the authentication message is valid.

21. The method of claim 20 further comprising:

generating a third key if the authentication message is determined to be valid.

22. The method of claim 20 further comprising:

generating key material if the authentication message is determined to be valid, wherein the key material may be

supplied to a function known to the first device and the mobile device to produce a third key.

23. The method of claim 20 wherein the authentication message comprises a hash of the request message, wherein the hash is computed using the first key.

24. The method of claim 20 wherein the request message comprises a Registration Request message.

25. The method of claim 23, wherein determining if the authentication message is valid comprises:

computing a hash of the request message using the first key; and

comparing the computed hash to the authentication message.

26. The method of claim 25 further comprising:

decrypting the data structure using the second key to obtain the first key.

27. The method of claim 21 further comprising:

receiving a reply message from the first device by the mobile device, wherein the reply message includes the third key.

28. The method of claim 27 further comprising:

forming a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network;

forming a second authentication message using the third key; and

transmitting the second request message and second authentication message to the first device.

29. A computer program product residing on a computer readable medium having instructions stored thereon that, when executed by the processor, cause that processor to:

form an authentication message comprising:

authentication data encrypted with a first key; and

the first key encrypted with a second key;

generate a request message requesting that datagrams destined for a first Internet Protocol address of a mobile device be routed to a second Internet Protocol address; and

include the authentication request message in the request message.

30. The computer program product of claim 29 wherein the authentication message comprises a Kerberos Application Request message.

31. The computer program product of claim 29 further comprising instructions to generate a hash of the request message using the first key to form a second authentication message.

32. The computer program product of claim 29 further comprising instructions to:

receive a reply message from the first device by the mobile device, wherein the reply message includes a third key;

form a second authentication message using the third key;

transmit a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network, wherein the second authentication message is included in the second request message.

33. A computer program product residing on a computer readable medium having instructions stored thereon that, when executed by the processor, cause that processor to:

extract an authentication message from a message requesting that datagrams destined for a first Internet Protocol address of a mobile device be routed to a second Internet Protocol address, wherein the authentication message comprises:

authentication data encrypted with a first key; and

a data structure comprising the first key, and encrypted with a second key;

verify the authentication data; and

if the authentication data is valid, then generating a third key.

34. The computer program product of claim 33 further comprising instructions that cause the processor to:

form a reply message that includes the third key; and

transmit the reply message to a device associated with the request message.

35. The computer program product of claim 33 further comprising instructions that cause the processor to:

store the encryption key.

36. The computer program product of claim 33 wherein the message comprises a Registration Request message.

37. A system comprising:

a first network device associated with a first network; and

a second network device associated with the first network, the second network device capable of:

producing an authentication message including a data structure comprising the first key with the data structure encrypted with a second key;

generating a request message to have the first network device deliver datagrams destined for a home address associated with the second device on the first network to a second address on a second, different network; and

including the authentication message within the request message.

38. The system of claim 37 wherein the second network device is further capable of forming a second authentication message by computing a hash of the request message using the first key.

39. The system of claim 38 wherein the first network device is capable of receiving the request message and generating a key if the second authentication message is valid.

40. The system of claim 37 wherein the first network device is a router.

41. The system of claim 37 wherein the second network device is a laptop computer.

42. The system of claim 37 further comprising:

a third device capable of producing the first key and the data structure encrypted with the second key.

43. A system comprising:

a router associated with a first network and comprising an input port for receiving datagrams and a switch fabric for determining destination of datagrams; and

a processor capable of:

reading request message to reroute datagrams destined for a first address of a mobile device associated with the first network to a second address associated with a second, different network, wherein the request message includes a data structure comprising a first key unknown to the processor encrypted with a second key that is known to the processor,

verifying an authentication message associated with the request message wherein the authentication message

comprises a hashed version of the request message computed using the first key; and

if the authentication message is valid, then generating a third key.

44. The system of claim 43, wherein the processor is further capable of:

encrypting the third key.

45. The system of claim 44, wherein the processor is further capable of:

forming a reply message, wherein the reply message includes the encrypted third key; and

forming a reply authentication message.

46 The method of claim 45 wherein the reply authentication message comprises a hashed version of the reply message.

47. The method of claim 45 further comprising: transmitting the reply message and the reply authentication message to the mobile device at the second address.